I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

MEGAN M. ENGLE*

# Anti-Spyware Enforcement: Recent Developments

**Abstract:** Spyware plagues computer users by installing itself on computers without user consent, and, among other things, changing browser settings and home pages, tracking users' online activities, causing unwanted pop-up ads, and making uninstallation extremely difficult, if not impossible. This note briefly reviews recent legislative efforts to combat spyware at both the state and federal levels, and summarizes the Federal Trade Commission's recent enforcement activities in this area.

* Megan M. Engle is a Juris Doctor candidate at The Ohio State University Moritz College of Law, Class of 2008. She earned Bachelor of Arts degrees in Topical Studies (Islamic Studies) and Psychology and graduated *magna cum laude* from the University of Kentucky. The author would like to thank two important people: Martha K. Landesberg for her invaluable guidance and Jesse L. Taylor for his unwavering support during the note writing process.

## I. INTRODUCTION

Despite technological advances and state and federal actions, spyware has become more elusive and problematic in 2007. A recent survey by the National Cyber Security Alliance and America Online, Inc. found that 80% of computers connected to the Internet have spyware or adware installed on them.[1] As a result, legislation and litigation are being pursued more aggressively to reduce the burden of spyware on home, business, and government computers.

Spyware is software placed on computers without the consent of the user, tracking online activity and often causing unwanted pop-up windows to appear.[2] The Anti-Spyware Coalition defines spyware (and other potentially unwanted technologies) as:

> technologies deployed without appropriate user consent and/or implemented in ways that impair user control over: material changes that affect their user experience, privacy, or system security; use of their system resources, including what programs are installed on their computers; and/or collection, use, and distribution of their personal or other sensitive information.[3]

Spyware is designed and offered by a number of providers. The spyware programs monitor user activities and transmit user information to remote servers and/or download unwanted targeted advertisements.[4]

---

[1] Brian Krebs, *Invasion of the Computer Snatchers*, WASH. POST, Feb. 19, 2006, at W10, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html.

[2] Jeremy Kirk, *Ad Dishes Up Adware to More Than a Million PCs*, PC WORLD, July 20, 2006, http://www.pcworld.com/article/id,126488-page,1-c,adware/article.html.

[3] Anti-Spyware Coalition, Anti-Spyware Coalition Definitions Document, http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm (last visited Jan. 26, 2008) (The Anti-Spyware Coalition identifies several types of spyware technologies, such as tracking software, advertising display software, remote control software, dialing software, system modifying software, security analysis software, automatic download software, and passive tracking technologies.).

[4] Benjamin Edelman, *"Spyware": Research, Testing, Legislation, and Suits*, http://www.benedelman.org/spyware/ (last visited Jan. 26, 2008).

Software programs defined as spyware engage in a wide range of surreptitious activities, including keystroke recorders, screen capture programs, and numerous additional software programs that alter computer settings, monitor users' online activities, transmit that information to third parties, and/or compromise computer performance.[5] Users spend inordinate amounts of time attempting to remove spyware, which is often designed to make uninstallation difficult, if not impossible. Websites that distribute spyware are often paid based on the number of computers infected with the malicious software, motivating hackers to find new ways to install the spyware without the consent of computer users.[6]

Legislators and enforcement agencies, at both the state and federal levels, have been working to address the problems of spyware and unwanted adware in the past year. This note briefly highlights state and federal legislative efforts and litigation in the states before it focuses on a series of cases brought by the Federal Trade Commission against purveyors of spyware and against adware companies that use extensive affiliate networks to distribute their software.

## II. STATE AND FEDERAL EFFORTS TO COMBAT SPYWARE

In 2006, anti-spyware legislation was enacted in Hawaii, Louisiana, Rhode Island, and Tennessee.[7] The following year, Arkansas and Virginia enacted anti-spyware legislation and, as of the writing of this note, legislation is pending in fourteen other states.[8]

---

[5] *Id.*

[6] Kirk, *supra* note 2.

[7] National Conference of State Legislatures, 2006 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware06.htm (last visited Jan. 26, 2008).

[8] National Conference of State Legislatures, 2007 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware07.htm (last visited Jan. 26, 2008) (The 14 states that have introduced spyware bills are: Arkansas, California, Illinois, Indiana, Iowa, Maine, Massachusetts, Michigan, Mississippi, Missouri, New York, Pennsylvania, Texas, and Virginia. Additionally, of the states that are currently considering spyware legislation, Illinois, Maine, Missouri, and New York are considering acts that protect consumers from the illegal use of spyware. Regarding states that have enacted spyware legislation in 2007, the Arkansas law relates briefly to funding to help offset state spyware monitoring fines, while Virginia's governor signed a more comprehensive bill that classifies key loggers, bots, and zombies as computer trespass crimes and makes it a felony for a person to install or cause to be installed or collect information through software capable of recording keystrokes on the computer of another.).

Several state attorneys general filed lawsuits against purveyors of spyware under state fraud, consumer protection laws, and, in some cases, under new anti-spyware statutes.[9] Specifically, in 2007, New York, Texas, California, and Washington targeted and pursued perpetrators of spyware.[10]

In 2007, three bills aimed at combating spyware were introduced in the 110th Congress, yet none have been enacted as of the writing of this note. House Resolution 964, the Securely Protect Yourself Against Cyber Trespass Act ("Spy Act") would prohibit egregious software activities, such as surreptitious key-stroke logging, resetting browser settings without user consent, and hijacking modems and browsers.[11] It would also require software companies to provide clear and conspicuous notice to users of how software functions and the consequences of downloading that software, to obtain consent for downloading and installing the software, and to provide an uninstall process that is both easy to use and that completely removes software from users' computers.[12] Violations would be treated as unfair and deceptive trade practices under Section 5 of the Federal Trade Commission Act.[13] House Resolution 964 was passed by the House, but it is awaiting Senate action.[14]

House Resolution 964 was the work of the House Energy and Commerce Committee. In March 2007, the House Judiciary Committee introduced its own anti-spyware bill, House Resolution 1525, the Internet Spyware (I-SPY) Prevention Act of 2007.[15] The bill would enhance penalties for unauthorized access of a protected

---

[9] CTR. FOR DEMOCRACY & TECH., SPYWARE ENFORCEMENT: A REPORT BY THE CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT) (Sept. 2007), http://www.cdt.org/privacy/spyware/20060626spyware-enforcement.php [hereinafter *Spyware Enforcement]*.

[10] Center for Democracy & Technology, Spyware Enforcement–State, http://www.cdt.org/privacy/spyware/20060626spyware-enforcement-state.php (last visited Jan. 26, 2008).

[11] Securely Protect Yourself Against Cyber Trespass Act, H.R. 964, 110th Cong. (2007).

[12] *Id.* § 3.

[13] *Id.*

[14] *Id.*

[15] Internet Spyware (I-SPY) Prevention Act of 2007, H.R. 1525, 110th Cong. (2007), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR01525:@@@L&summ2=m&.

computer[16] under the Computer Fraud and Abuse Act,[17] and includes a "sense of Congress" provision, stating that the Department of Justice should use "[the] act, and all other available tools, to vigorously prosecute those who use spyware to commit crimes. . . ."[18] House Resolution 1525 passed the House in May 2007 and has been referred to the Senate Judiciary Committee. The Senate has its own version of anti-spyware legislation. In June 2007, Senator David Pryor introduced legislation that would require notice and consent for software downloads. The measure is pending in the Senate Committee on Commerce, Science, and Transportation.[19]

## III. FEDERAL TRADE COMMISSION ENFORCEMENT EFFORTS

The Federal Trade Commission ("FTC") has been the most aggressive federal agency in the fight against spyware in the past year.[20] As of September 2007, the FTC brought eleven spyware-

---

[16] *Id.* (A person who intentionally gains unauthorized access, or exceeds their authorized access, to a protected computer by causing a program or code to be transmitted onto the computer and intentionally uses the program in furtherance of another federal criminal offense could face a fine and up to five years in jail. A lesser fine and prison sentence of up to two years would be imposed if the unauthorized access is gained for either of the following: intentionally obtaining or transmitting personal information with intent to defraud or injure a person or cause damage to a protected computer; or intentionally impairing the security protection of a protected computer with the intent to defraud or injure a person or damage such computer.).

[17] Matt Hines, *Policy Experts Split on Spyware Laws: CDT and FTC Disagree Whether a Trio of Anti-Spyware Bills Before Congress Will Result in More Prosecutions*, INFOWORLD, June 28, 2007, http://www.infoworld.com/article/07/06/28/Policy-experts-split-on-spyware-laws_1.html.

[18] H.R. 1525 § 4.

[19] Counter Spy Act, S.1625, 110th Cong. (2007). The bill would prohibit a person who is not an authorized user of a protected computer from installing software that takes control of the computer, modifies the computer's settings, or prevents the user's efforts to block installation of, disable, or uninstall software. It would also prohibit such installation of software that collects sensitive personal information without first providing clear and conspicuous disclosure to the authorized user and obtaining the user's consent. The proposed Act would prohibit installation of adware on a protected computer, unless the source is clear and instructions for uninstallation are provided, or the advertisements are displayed exclusively when the software author or publisher's website or online service is used. A number of exceptions are found in the bill, including those for computer security, diagnostics, technical support, detection of unauthorized use of fraudulent software, and other illegal activities.

[20] The Department of Justice has filed complaints against perpetrators of spyware under the Computer Fraud and Abuse Act and the Wiretap Act, with 11 cases to date; none were filed in

related cases under Section 5 of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair and deceptive commercial practices.[21] The following is a discussion of the most recent of these cases, some against purveyors of spyware, others against distributors of adware.

The FTC obtained stipulated permanent injunctions, effectively shutting down the business operations of several spyware providers in 2007. In its case against Odysseus Marketing, Inc. and its principal, Walter Rines, the FTC alleged that the defendants' online advertisements for software that would allow anonymous peer-to-peer file sharing, using claims like "DOWNLOAD MUSIC WITHOUT FEAR" and "DON'T LET THE RECORD COMPANIES WIN," were false and misleading because the software did not, in fact, make peer-to-peer file sharing anonymous.[22]

Additionally, the FTC alleged that the software was bundled with "Clientman," a hidden spyware program that surreptitiously downloaded dozens of other software programs, including some that reformatted search engine results in favor of defendants' clients.[23] The complaint further alleged that Clientman collected consumers' personal information and installed third-party software that delivered pop-ups and other advertisements to consumers without first notifying them.[24] Moreover, the Clientman software exploited browser security vulnerabilities in order to download material to the consumer computers.[25]

The FTC alleged that Odysseus Marketing violated Section 5(a) of the FTC Act by unfairly and deceptively infecting computers of

---

2007, however. *Spyware Enforcement*, *supra* note 9. The Center for Democracy and Technology maintains a list of cases the Department of Justice has brought from 2005 to the present. The Department of Justice also maintains a database of recently prosecuted computer crimes dating from 1998. Department of Justice, Computer Crime Cases, http://www.usdoj.gov/criminal/cybercrime/cccases.html (last visited Jan. 26, 2008).

[21] *Spyware Enforcement*, *supra* note 9 (The FTC also maintains a spyware page that has educational materials for consumers and a list of FTC enforcement actions at http://www.ftc.gov/spyware).

[22] First Amended Complaint for Injunction and Other Equitable Relief ¶ 35, FTC v. Odysseus Marketing, Inc., Civil No. 05-CV-330-SM (D.N.H. Mar. 24, 2006), *available at* http://www.ftc.gov/os/caselist/0423205/060504amendedcmplt.pdf.

[23] *Id.* ¶¶ 8, 13.

[24] *Id.*

[25] *Id.* ¶¶ 9–10.

unknowing consumers with multiple spyware programs.[26] The Commission's willingness to use its "unfairness" authority in this case is noteworthy. Specifically, the Commission alleged that the download and installation of Clientman software onto consumers' computers without their knowledge or consent, and the subsequent collection of their personal information, was unfair.[27] As a result of the downloads, consumers were forced to spend substantial time and money attempting to prohibit further collection of personal information, and to rectify damage done to their computers' performance caused by the software. These problems, though, could not be rectified, and the Clientman software could neither be located nor uninstalled through reasonable means. Therefore, consumers could not reasonably avoid the harm caused by the software, and the defendants' actions were thus "unfair" within the meaning of the FTC Act.[28] The FTC's deceptiveness claims stemmed from the defendants' alleged failure to disclose the bundling of Clientman with their purported file-sharing software and their false representations to consumers that the software would provide anonymity for file sharing.[29]

In October 2006, the FTC and defendants entered into a stipulated order and settlement, which prohibited the defendants from (1) downloading software onto consumers' computers without notice and consent, (2) exploiting security vulnerabilities to download and install software, (3) misrepresenting what their software does and how it works, and (4) collecting personal information without notice and consent.[30] The order required defendants to disclose any future software downloads to consumers and to provide an effective uninstall mechanism.[31] Finally, Odysseus was required to pay $1.75 million in

---

[26] *Id.* ¶¶ 34, 37, 40, 43.

[27] *Id.* ¶¶ 31–34.

[28] *Id.* ¶¶ 41–43.

[29] *Id.* ¶¶ 38–40.

[30] Stipulated Final Order for Permanent Injunction and Settlement of Claims for Monetary Relief at 8–12, FTC v. Odysseus Marketing, Inc. (D.N.H. Oct. 24, 2006), *available at* http://www.ftc.gov/os/caselist/0423205/061121odysseusstipfinal.pdf.

[31] *Id.* at 8–17. The FTC alleged that, rather than remove the software, the defendants' uninstall mechanism actually downloaded more software programs.

equitable relief; all but $10,000 of which was suspended because the defendants were unable to pay.[32]

The Commission's case against ERG Ventures, LLC, a spyware provider, its principals, and an affiliate distributor, follows the pattern set by *FTC v. Odysseus Marketing, Inc.*[33] The Commission alleged that the defendants misled consumers into downloading a package of malicious software programs on consumers' computers by hiding it in seemingly harmless and free software, such as screensaver programs and video files.[34] The Media Motor Application package downloaded malware that, among other things, changed consumers' default homepages, tracked consumers' online activities, added difficult-to-remove toolbars displaying pop-up ads that included pornography, altered browser settings, and degraded the performance of consumers' computers.[35] Additionally, the complaint alleged that many of the downloaded malware programs were difficult or impossible to remove, and still others disabled anti-spyware software on users' computer further contributing to the harms sustained by consumers.[36]

As in *Odysseus Marketing,* the FTC in *FTC v. ERG Ventures* alleged claims of both deception and unfairness under Section 5 of the FTC Act.[37] The deceptiveness claims stemmed from the defendants' failure to alert consumers that the free software was bundled with the Media Motor Application, and defendants' false representation in an End User License Agreement ("EULA"). The EULA alleged that consumers could prevent the installation of malware on their computers by clicking a "cancel" button. The unfairness claims were based on the substantial harm to consumers caused by the Media Motor Application software.[38] Because the software was downloaded

---

[32] *Id.* at 16.

[33] Complaint for Injunctive and Other Equitable Relief, FTC v. ERG Ventures, LLC, No. 3:06-CV-00578-LRH-VPC (D. Nev. Oct. 30, 2006), *available at* http://www.ftc.gov/os/caselist/0623192/061030ergventurescmplt.pdf.

[34] *Id.*¶ 15. The FTC initially sought and was granted a temporary restraining order ("TRO"). The FTC also sought the TRO to temporarily freeze ERG's assets, requiring the defendants to prepare an accounting of their assets and ordering the defendants to preserve their business records and provide other equitable relief that is in the public interest. *Id.*

[35] *Id.* ¶ 17.

[36] *Id.* ¶¶ 38–40.

[37] *Id.* ¶¶ 52, 55, 58, 61, 65.

[38] *Id.* ¶¶ 56–58.

surreptitiously and could not be removed even if discovered, the ensuing harms could not have been reasonably avoided by consumers.[39]

In October 2007, the FTC and ERG Ventures entered into a stipulated final order that prohibited the defendants from downloading software onto consumer computers without consent or downloading software that interferes with computer use.[40] The order also required the defendants to fully disclose the name and function of all software they install on consumers' computers, to offer consumers the ability to cancel installation after reviewing the disclosure, and to provide an effective and transparent uninstall mechanism.[41] Finally, the defendants were required to pay $330,000 to the Commission as consumer redress.[42]

The Commission's cases against Enternet Media, Inc.[43] and Digital Enterprises, Inc.[44] echo the issues raised in the earlier spyware cases. In *FTC v. Enternet Media Inc.*, the defendants bundled free software downloads with software that served pop-up ads containing purported free browser and security upgrades. The complaint alleged that the free upgrade software surreptitiously tracked users' online activities, changed their default home pages, inserted new toolbars and other software that could not be uninstalled, generated pop-up ads, and degraded computer functionality.[45] The *Enternet Media* defendants

---

[39] *Id.* ¶¶ 43–48.

[40] Stipulated Final Order for Permanent Injunction and Monetary Judgment as to Defendants ERG Ventures, LLC, Elliott S. Cameron, Robert A. Davidson, II, and Garry E. Hill, FTC v. ERG Ventures, LLC, No. 3:06-CV-00578-HDM-VPC, (D. Nev. Oct. 3, 2007), *available at* http://www.ftc.gov/os/caselist/0623192/070928ergventursestipfinal.pdf.

[41] *Id.*

[42] *Id.* at 7.

[43] First Amended Complaint for Injunctive and Other Equitable Relief, FTC v. Enternet Media, Inc., No. CV05-7777 CAS AJWx (C.D. Cal. Nov. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0523135/051110amndcomp0523135.pdf [hereinafter *Enternet Media Complaint*].

[44] Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Digital Enterprises, Inc., No. CV06-4923 CAS AJWx (C.D. Cal. Aug. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0623008/060808movielandcmplt.pdf [hereinafter *Digital Enterprises Complaint*].

[45] *Enternet Media Complaint*, *supra* note 43, ¶ 12.

included both the providers of the software and a webmaster affiliate through which the surreptitious software was distributed.[46]

The defendants in *FTC v. Digital Enterprises, Inc.* were the owners of three websites through which software serving particularly intrusive pop-up advertisements was downloaded without notice or consent.[47] The complaint alleged that the Digital Enterprises software bombarded consumers with large, noisy pop-ups, often lasting close to a minute, which could not be manually closed or exited by the consumer.[48] According to the Commission, the pop-ups falsely claimed that consumers had signed up for a three-day trial period for Digital Enterprises' software download service and failed to cancel before the deadline, thereby incurring a $99 fee. Consumers who tried to remove the software from the Windows control panel "add/remove programs" screen were redirected to a website that demanded the $99 fee to stop the pop-ups.[49] In many cases, consumers were only able to stop the pop-ups by paying the fee demanded.[50]

*Enternet Media* and *Digital Enterprises* involved claims of both unfairness and deception. Misrepresentations as to the true nature of the downloaded software gave rise to the Commission's deception claims. In each case, the Commission reiterated that surreptitious installation of software that harms computers and cannot be removed by reasonable means is an unfair trade practice.[51] In *Digital Enterprises*, the defendant's demand that consumers pay to stop the pop-ups was also alleged to be an unfair practice. Each case ended in 2007 with a stipulated permanent injunction and an order prohibiting the defendants from, among other things, downloading software without notice and consumer consent, and without providing an effective uninstall mechanism.[52] The orders also included significant

---

[46] *Id.* ¶¶ 5–10.

[47] *Digital Enterprises Complaint*, *supra* note 44, ¶¶ 6–18.

[48] *Id.* ¶ 51.

[49] *Id.* fig. 4.

[50] *Id.* ¶ 37.

[51] *Enternet Media Complaint*, *supra* note 43, ¶¶ 44–46; *Digital Enterprises Complaint*, *supra* note 44, ¶¶ 54–56.

[52] Stipulated Final Order for Permanent Injunction and Monetary Judgment as to Defendants Enternet Media, Inc., Conspy & Co., Inc., Lida Rohbani, Nima Hakimi, and Baback (Babak) Hakimi, FTC v. Enternet Media, Inc., No. CV05-7777 CAS AJW, (C.D. Cal. Aug. 23, 2006),

monetary judgments against the defendants. Enternet Media and its principals were required to pay $8,500,000, all but $2,045,000 of which was suspended;[53] Digital Enterprises was required to pay $500,000 in consumer redress.[54]

In addition to obtaining an injunction in the case discussed above, the Federal Trade Commission entered into two significant settlements in 2007 with providers and distributors of advertising software ("adware") that used extensive affiliate networks to distribute their software by surreptitiously bundling it with various types of free software. These settlements are significant not only because they reiterate the Commission's position on "unfairness" and "deception" within the meaning of the FTC Act, but also because they hold the adware companies responsible for the actions of the affiliates in their distribution networks.

In its case against Zango, Inc., the Commission alleged that Zango used a network of affiliates (who recruited sub-affiliates) to distribute its adware by bundling it with "lureware" (including free browser upgrades, utilities, screen savers, games, peer-to-peer file sharing, and/or entertainment content) installed on consumers' computers.[55] The bundling took place either with inadequate notice (e.g., through inconspicuous hyperlinks) or without any notice to consumers. Once installed, the adware tracked consumers' Internet activity and bombarded them with targeted pop-up ads.[56] Moreover, the

---

*available at* http://www.ftc.gov/os/caselist/0523135/060823enternetmediastlmnt.pdf [hereinafter *Enternet Media Final Order*]; Settlement Agreement and Stipulated Final Order for Permanent Injunction and Monetary Relief, FTC v. Digital Enterprises, Inc., No. CV06-4923 CAS AJWx (C.D. Cal. Sept. 5, 2007), *available at* http://www.ftc.gov/os/caselist/0623008/070905digitalenterprisesstipfnl.pdf [hereinafter *Digital Enterprises Final Order*].

[53] *Enternet Media Final Order*, *supra* note 52, at 8–9. The Commission entered into a separate stipulated order and permanent injunction against Nicholas Albert, Enternet Media's affiliate. Stipulated Final Order for Permanent Injunction and Monetary Judgment as to Defendant Nicholas C. Albert, FTC v. Enternet Media, Inc., No. CV05-7777 CAS AJWx (C.D. Cal. Dec. 14, 2006), *available at* http://www.ftc.gov/os/caselist/0523135/061214enternetmediaalbertstlmnt.pdf [hereinafter *Enternet Media Stipulated Order with Albert*]. The order prohibits Albert from interfering with consumers' use of their computers and from misrepresenting the nature of software downloaded from his Website, and requires him to pay $3,300 as disgorgement. *Id.* at 7–9.

[54] *Digital Enterprises Final Order*, *supra* note 52, at 13–14.

[55] Complaint ¶10, *In re* Zango, Inc., Docket No. C-4186, (FTC Nov. 3, 2006), *available at* http://www.ftc.gov/os/caselist/0523130/0523130cmp061103.pdf [hereinafter *Zango Complaint*].

[56] *Id.* ¶ 6.

Commission alleged that the adware could not be reasonably identified, located, or removed by consumers, because Zango designed it to be extremely difficult to locate or uninstall.[57] For example, Zango failed to name the source of the adware in the pop-up ads, obfuscated the name of the software in the Windows "add/remove programs" function, and provided an "uninstall mechanism" that did not remove the software.[58]

The Commission's claims in *Zango* were substantially similar to those in its subsequent case against Direct Revenue, LLC, which marketed and distributed its adware on its own websites and through an extensive network of affiliates and sub-affiliates.[59] According to the Commission, Direct Revenue's adware was bundled with "lureware," such as free games and screensavers, and installed (either by Direct Revenue or by its affiliates) on consumers' computers with little or no notice, or consent.[60] The Commission also alleged that Direct Revenue designed the adware to be difficult, if not impossible, to identify, locate, and uninstall.[61]

The *Zango* and *Direct Revenue* matters included deceptiveness and unfairness claims. The Commission alleged that offering "lureware" without disclosing that it is bundled with adware was a deceptive trade practice, because the fact that the adware tracked online activities and served pop-up ads would be material to consumers' decisions whether to install the free software and content in the first place.[62] In each case, the Commission also alleged that the installation of adware, without notice or consent, that could not reasonably be identified as adware, was an unfair trade practice, whether it was located on the computer or had been uninstalled by consumers. The Commission alleged that the failure to provide a reasonable means to identify, locate, or uninstall the adware is an unfair trade practice in itself.[63]

---

[57] *Id.* ¶ 14.

[58] *Id.*

[59] Complaint ¶10, *In re* Direct Revenue, LLC, Docket No. C-4194, (FTC June 29, 2007) *available at* http://www.ftc.gov/os/caselist/0523131/0523131cmp070629.pdf [hereinafter *Direct Revenue Complaint*].

[60] *Id.* ¶ 12.

[61] *Id.* ¶ 15.

[62] *Zango Complaint, supra* note 55, ¶ 16; *Direct Revenue Complaint, supra* note 58, ¶ 16.

[63] *Zango Complaint, supra* note 55, ¶ 18; *Direct Revenue Complaint, supra* note 58, ¶ 18.

Finally, the Commission alleged that these practices have or were likely to cause substantial consumer injury (in time or money spent in locating and removing unwanted adware) that consumers could not have reasonably avoided and that is not outweighed by benefits to consumers or competition.[64]

The *Zango* and *Direct Revenue* settlements were substantially similar.[65] Each required significant payments to the Federal Trade Commission ($3,000,000 and $1,500,000, respectively).[66] The settlements require each company to obtain "express consent" for future download and installation of its adware. "Express consent" included both clear and conspicuous notice *outside* the End User License Agreement of the "material terms" of the software (including how it functions) and an affirmative step by the consumer, such as clicking on a clearly labeled "install" or "download" hyperlink to indicate consent.[67] Advertisements must be labeled with the name of the software program serving them and must also include a clearly labeled, direct hyperlink to instructions on how to submit complaints and uninstall the adware.[68] The settlements also required Zango and Direct Revenue to provide a clear notice and a functioning e-mail or Internet-based mechanism for consumer complaints (and to promptly investigate those complaints) and an effective uninstall mechanism that can be easily located (e.g., in the operating system's add/remove prgrams list).[69]

Perhaps most significant, however, are the settlement provisions holding Zango and Direct Revenue accountable for the practices of

---

[64] *Zango Complaint*, *supra* note 55, ¶ 17; *Direct Revenue Complaint*, *supra* note 58, ¶ 17.

[65] Decision and Order, In the Matter of Zango, Inc., Docket No. C-4168 (FTC Mar. 7, 2007), *available at* http://www.ftc.gov/os/caselist/0523130/0523130c4186decisionorder.pdf [hereinafter *Zango Decision and Order*]; Decision and Order, In the Matter of DirectRevenue, LLC, Docket No. C-4194 (FTC June 26, 2007), *available at* http://www.ftc.gov/os/caselist/0523131/0523131do070629.pdf [hereinafter *Direct Revenue Decision and Order*].

[66] *Zango Decision and Order*, *supra* note 65, at 8; *Direct Revenue Decision and Order*, *supra* note 65, at 8.

[67] *Zango Decision and Order*, *supra* note 65, at 3; *Direct Revenue Decision and Order*, *supra* note 65, at 3–4.

[68] *Zango Decision and Order*, *supra* note 65, at 7; *Direct Revenue Decision and Order*, *supra* note 65, at 7–8.

[69] *Zango Decision and Order*, *supra* note 65, at 4–5, 7; *Direct Revenue Decision and Order*, *supra* note 65, at 6, 8.

their affiliates and distribution networks. Each company must have a "comprehensive program reasonably designed to ensure" that affiliates obtain consumers' "express consent" prior to installing their adware on consumers' computers.[70] To do so, each company must obtain contact and bank account information for each of its affiliates, and require them to sign an agreement to comply with the settlement terms. Affiliates must be on notice that their failure to comply will result in termination from the affiliate network.[71] Each company's affiliates must, in turn, impose the same requirements upon their sub-affiliates and sub-contractors.[72]

## IV. CONCLUSION

As the discussion at the 2007 Federal Trade Commission "Spam Summit" demonstrates,[73] the flood of spyware, and other malicious software delivered by e-mail, is not likely to abate any time soon. The states have enacted a patchwork of legal tools to combat spyware, but the federal government has yet to enact a national enforcement standard. The Federal Trade Commission has stepped in, using its existing authority under the FTC Act to sue spyware providers and distributors for unfair and deceptive trade practices, in many cases shutting down spyware operations entirely. In the absence of federal legislation specifically targeted at spyware, the Commission's enforcement efforts are essential in the battle against those who have taken advantage of the Internet's open architecture to invade consumers' computers with unwanted or destructive software.

---

[70] *Zango Decision and Order*, *supra* note 65, at 5–6; *Direct Revenue Decision and Order*, *supra* note 65, at 6–7.

[71] *Zango Decision and Order*, *supra* note 65, at 5; *Direct Revenue Decision and Order*, *supra* note 65, at 7.

[72] *Zango Decision and Order*, *supra* note 65, at 5–6; *Direct Revenue Decision and Order*, *supra* note 65, at 7.

[73] FTC, Spam Summit, http://www.ftc.gov/bcp/workshops/spamsummit/index.shtml (last visited Jan. 26, 2008).